Emergency Action Plan Guide
Active Shooter Preparedness

Purpose

The Active Shooter Emergency Action Plan Video is a virtual learning tool that describes the fundamental concepts of developing an Emergency Action Plan (EAP) for an active shooter scenario. This instructive video guides organizations through important considerations of EAP development utilizing the first-hand perspectives of active shooter survivors, first responders, and other subject matter experts who share their unique insights.

Organizations are encouraged to use this guide as a medium to document the *initial steps* toward creating an Active Shooter preparedness plan. This guide *is not* meant to replace your organization's Emergency Action Plan. Rather, it is a tool that begins the EAP development process.

Pre-Planning Recommendations and Suggested Training

- ✓ Does your organization have an emergency action plan? If so, review your organization's policy or process for creating the plan. Determine if an active shooter preparedness plan can fit into your organization's overarching plan which may already include a plan for fire evacuation, severe weather, and bomb threats.
- ✓ Obtain a copy of the Federal Emergency Management Agency's (FEMA) Comprehensive Preparedness Guide (CPG) 101 *"Developing and Maintaining Emergency Operations Plan"* and review the six step planning process.
- ✓ Explore the Department of Homeland Security's Active Shooter Preparedness Website to better understand the active shooter threat.
- ✓ View the Options for Consideration Video to recognize possible actions to take if confronted with an active shooter scenario.
- ✓ Download and review the Active Shooter Preparedness Workshop Series presentations. This six module series contains additional information, instructor notes, and videos that supports the Active Shooter Emergency Action Plan process. The *Planning Steps (1-6)* below will correlate to the Training Modules (1-6) in the presentation slides. *Example: Module 2 will assist with completing Planning Step 2a and 2b.*

How to Use This Guide

Step 1 – Review the pre-planning recommendations and suggested training.

Step 2 – Allot *at least* **2-hours** to complete the Active Shooter Emergency Action Plan video.

Step 3 – Watch the EAP video.

Step 4 – Complete ***Planning Steps 1-6***. Use the fillable space to document the initial steps required to begin developing the organization's Emergency Action Plan. Note: *The Planning Steps contain information derived from the EAP video and other online resources to help inform the planning process.*

Step 5 – Begin drafting the organization's Active Shooter Emergency Action Plan. Refer to the EAP Guide and resources listed in *Pre-Planning Recommendations and Suggested Training* as required.

Need Help? Contact the DHS Active Shooter Preparedness team at ASworkshop@hq.dhs.gov

Planning Step - 1

Form a Collaborative Planning Team

Identify a cross-section of employees to represent your organization. The members should represent a broad perspective and include key segments of the organization. It is recommended that teams contain at least four members to ensure diversity of awareness and less than 10 members to avoid an unmanageable group. The positions listed below are examples of collaborative planning team members. Refer to *CPG 101 page 4-2* for additional information.

Human Resources	Information Technology Managers
Security, Risk or Safety Managers	Legal Advisors
Facility Managers or Engineers	Persons with Disabilities or Functional Needs
First Responders (Police, Fire/EMS)	Communication Managers

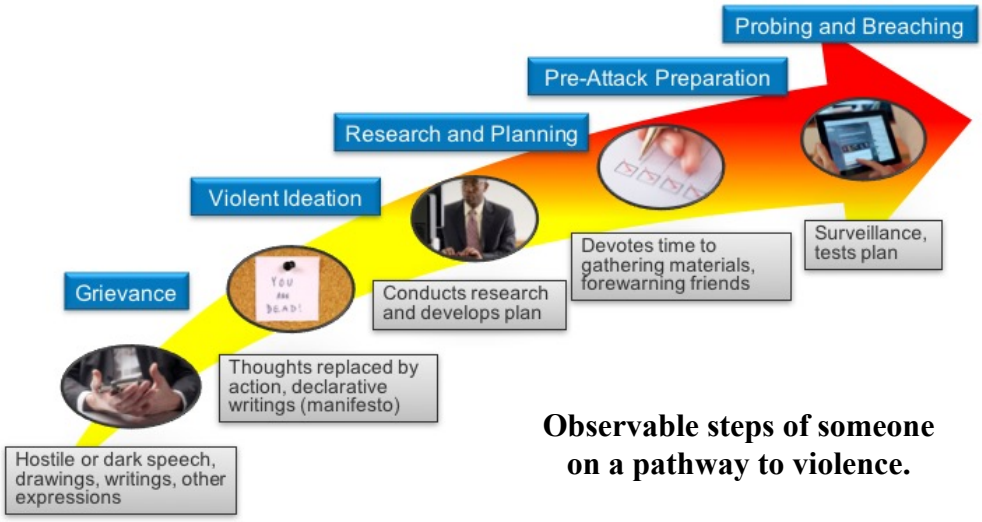
Position	Name	Contact Information

Planning Step – 2a

Develop an Active Shooter Prevention Plan

Effective prevention capabilities encompass three areas: training employees to recognize behaviors on the Pathway to Violence, a system for reporting that is tailored to your organization, and development of intervention capabilities that are trained and resourced to appropriately evaluate potential threats.

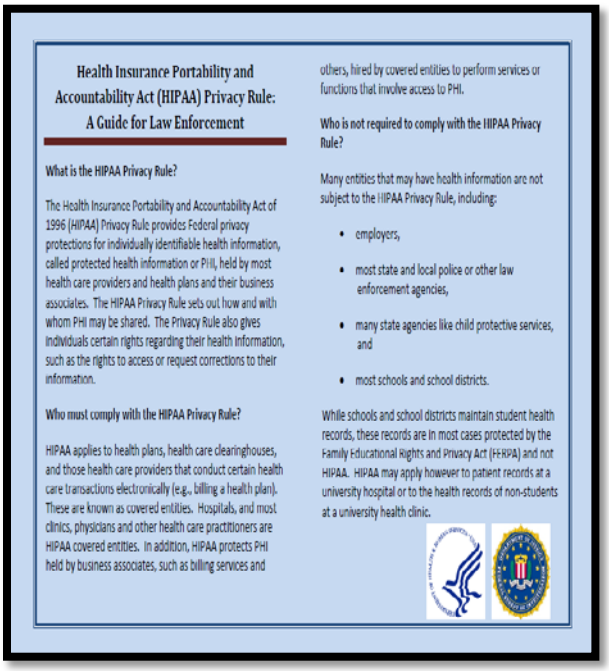
Pathway to Violence Training: The Pathway to Violence Video provides information regarding the behavior indicators that assailants often demonstrate before a violent act. It includes law enforcement expert interviews that discusses engagement strategies and recommended responses. Organizations can also refer to the Pathway to Violence Fact Sheet for additional information. Describe how you will train your organization to recognize the indicators of someone on a pathway to violence.



Observable steps of someone on a pathway to violence.

Reporting Mechanism: Describe the reporting process for your organization. Consider the types of information reportable to supervisors, security, human resources and law enforcement. How will employees know about the reporting process (policy, training, etc.)? How can the organization develop a culture of reporting?

Note: It's very important to consult with legal advisors throughout the planning process. For example, *The Health Insurance Portability and Accountability Act (HIPPA)* and *Family Education Rights and Privacy Act (FERPA)* both have ***exceptions*** that allow for information sharing to protect the health and safety of individuals.



Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement

What is the HIPAA Privacy Rule?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule provides Federal privacy protections for individually identifiable health information, called protected health information or PHI, held by most health care providers and health plans and their business associates. The HIPAA Privacy Rule sets out how and with whom PHI may be shared. The Privacy Rule also gives individuals certain rights regarding their health information, such as the rights to access or request corrections to their information.

Who must comply with the HIPAA Privacy Rule?

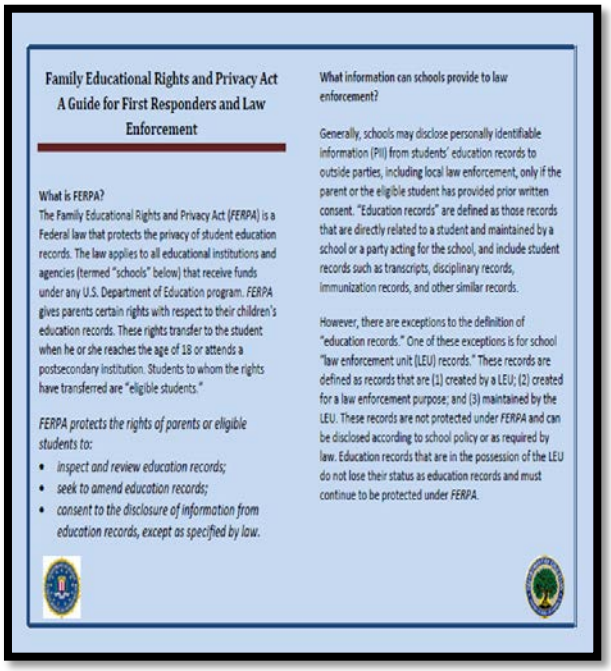
HIPAA applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (e.g., billing a health plan). These are known as covered entities. Hospitals, and most clinics, physicians and other health care practitioners are HIPAA covered entities. In addition, HIPAA protects PHI held by business associates, such as billing services and others, hired by covered entities to perform services or functions that involve access to PHI.

Who is not required to comply with the HIPAA Privacy Rule?

Many entities that may have health information are not subject to the HIPAA Privacy Rule, including:

- employers,
- most state and local police or other law enforcement agencies,
- many state agencies like child protective services, and
- most schools and school districts.

While schools and school districts maintain student health records, these records are in most cases protected by the Family Educational Rights and Privacy Act (FERPA) and not HIPAA. HIPAA may apply however to patient records at a university hospital or to the health records of non-students at a university health clinic.



Family Educational Rights and Privacy Act A Guide for First Responders and Law Enforcement

What is FERPA?

The Family Educational Rights and Privacy Act (*FERPA*) is a Federal law that protects the privacy of student education records. The law applies to all educational institutions and agencies (termed "schools" below) that receive funds under any U.S. Department of Education program. *FERPA* gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a postsecondary institution. Students to whom the rights have transferred are "eligible students."

FERPA protects the rights of parents or eligible students to:

- *inspect and review education records;*
- *seek to amend education records;*
- *consent to the disclosure of information from education records, except as specified by law.*

What information can schools provide to law enforcement?

Generally, schools may disclose personally identifiable information (PII) from students' education records to outside parties, including local law enforcement, only if the parent or the eligible student has provided prior written consent. "Education records" are defined as those records that are directly related to a student and maintained by a school or a party acting for the school, and include student records such as transcripts, disciplinary records, immunization records, and other similar records.

However, there are exceptions to the definition of "education records." One of these exceptions is for school "law enforcement unit (LEU) records." These records are defined as records that are (1) created by a LEU; (2) created for a law enforcement purpose; and (3) maintained by the LEU. These records are not protected under *FERPA* and can be disclosed according to school policy or as required by law. Education records that are in the possession of the LEU do not lose their status as education records and must continue to be protected under *FERPA*.

Intervention Resources: Describe your organization's process to intervene early and prevent violence.

Does your organization have a Threat Management Team (TMT) to conduct threat evaluations? If not, who should be on your team and how will they be trained? Consider including members from security, human resources, employee assistance and mental health. Learn more about TMT in the Federal Bureau of Investigation's "Making Prevention a Reality: Identifying, Assessing and Managing the Threat of Targeted Attacks" chapter 5.

Threat Management Team / Intervention Resources

Position	Name	Contact Information

Planning Step – 2b

Conduct a Risk Assessment

Organizations should consider all *threats*, *vulnerabilities* and associated *consequences* during their risk assessment. FEMA's CPG 201 "Threat and Hazard Identification and Risk Assessment Guide" is an effective resource to use when conducting risk assessments. Conducting a risk assessment will ensure organizations understand their situation, prioritize their actions, identify and compare options, and effectively allocate their resources.

An important threat for organizations to consider is *Workplace Violence*. Having an effective workplace violence policy can protect lives and prevent legal liability. Ensure your policy supports the Occupational Safety and Health's General Duty Clause.

Estimate the Risk Factors your organization faces:

Do you operate a controversial business?	Do you have security measures on-site or off-site?
Does your business have high-stress positions?	What is your organizations security protocols?
Do you have a history of work place violence or prior threats / incidents?	What is your work environment? (open access to the public, large crowds, high-risk neighbors)

List prior threats and violent incidents:

What is the most likely type of Workplace Violence your organization may encounter? Type 1

TYPE 1: Violent acts by criminals who have no other connection with the workplace, but enter to commit robbery or another crime.

TYPE 2: Violence directed at employees by customers, clients, patients, students, inmates, or any others for whom an organization provides services.

TYPE 3: Violence against coworkers, supervisors, or managers by a present or former employee.

TYPE 4: Violence committed in the workplace by someone who doesn't work there, but has a personal relationship with an employee—an abusive spouse or domestic partner.

Planning Step - 3

Establish Goals and Objectives

Goals are broad statements of what personnel, equipment and resources are supposed to achieve. Objectives lead to achieving goals and determining the actions that participants in the process must accomplish. Goals and objectives are key to determining operational priorities and resources required to achieve a needed capability.

Active Shooter preparedness goals and objectives may vary depending on an organization's security posture, physical environment and available resources. Consider the following to determine what goals and objectives are needed in your organization. Use the space provided to describe additional goals and objectives.

Access control

- Updated access rosters
- Lockdown procedures
- Shelter in place (door locks)

Notification

- Employees
- Visitors
- Disabled (Seeing / Hearing impaired)
- Non-English speakers

Evacuation

- Routes
- People with disabilities
- Rally points

Emergency responder coordination

- Organization liaison
- Go-bags (facility maps, master keys, etc)

Accountability

- Reporting procedures

Communications management

- First responders / incident commander
- Survivors
- Family
- Media

Short-term recovery

- Hours
- Days
- Weeks

Long-term recovery

- Months
- Years
- Anniversary

Describe a security/response goal and objective. Include the resources your organization needs to achieve the goals (without regard for the resource availability). CPG-101 (page 4-11)

Goal

Objective

Resource

Example:

Goal: *Achieve 100% notification and acknowledgement of Run-Hide-Fight message among all personnel. Conduct immediate accessible messaging or notification by all methods, including texting and pop-up notification on the computer.*

Objective: *Immediately initiate emergency notification protocol, to include proliferation of Run-Hide-Fight message via all available mediums, such as telephone, pager, email, SMS, MMS, public announcements systems, desktop/website banners, social media, etc. Encourage acknowledgment of message when feasible/prudent for accountability purposes. Utilize all communications methods to notify all persons of an active shooter incident within a short period onset.*

Resource: *Accessible notification software, public address system, captioning, outgoing texting through emergency notification in the area. New technologies being developed that may be applicable.*

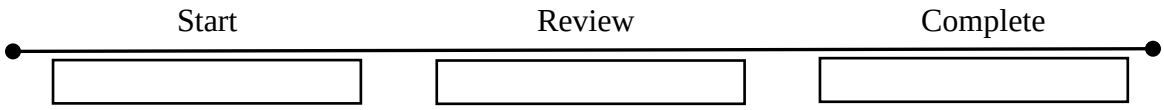
Planning Step - 4

Assess Courses of Action

Organizations must develop and analyze courses of action (COA) that accomplish specific goals and objectives. The COA should have a desired outcome that is measurable and incorporates an organization-wide focus. Assign the COA development to a member of the organization and include a timeline with decision points.

Describe at least two courses of action supporting the goal and objective listed in *Planning Step – 3* along with an anticipated timeline. CPG-101 (page 4-12)

Timeline: Establish preliminary start, review, and completion dates to establish expected timeframe.



COA #1 – Assigned to:

COA #2 – Assigned to:

Example:

COA 1: *Utilize computer screen with real-time caption pop-up announcements, "All-Call" alert for staff.*

COA 2 : *Sent a text to all employees "Run, Hide, Fight – Active Shooter on premises".*

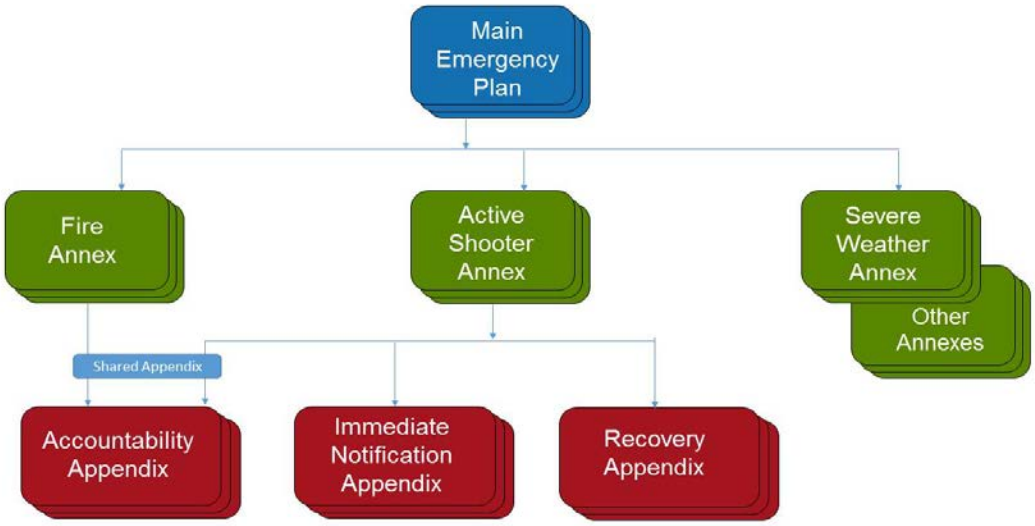
Planning Step - 5

Draft Plan and Approve

A planning team's main concern is to develop an Emergency Action Plan that includes all essential information and instructions that protect against an Active Shooter. CPG 101 (pages 3-1 & 4-16) recommends a format that users understand, are comfortable with, and can extract the information they need. Organizations are encouraged to use the Active Shooter Emergency Action Plan Template if they do not have an established format.

Draft the Plan

Determine if the Active Shooter plan will stand alone or supplement a main emergency plan. As seen below, organizations typically have a main emergency plan with annexes that cover specific hazards.

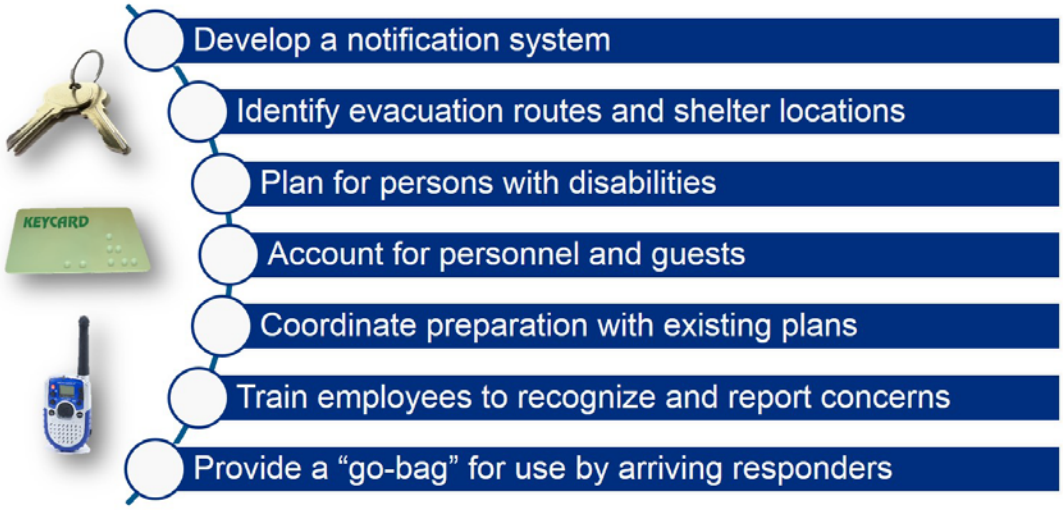


Recommended Rules for Drafting Plans – CPG 101 (page 4-16)

- Keep the language simple and use short sentences in active voice.
- Summarize important information with checklists and visual aids, such as maps and flowcharts.
- Avoid using jargon and minimize the use of acronyms.
- Provide enough detail to convey an easily understood plan that is actionable.
- Format the plan so that readers can quickly find solutions and options.
- Provide mission guidance and avoid discussing policy.
- Ensure accessibility by developing alternate formats: e.g. print, electronic, video.

Validate the Plan and Prepare for Approval – CPG 101 (page 4-17)

Check to ensure the written plan supports all goals and objectives developed by the planning group. Coordinate with a legal adviser to confirm plan supports all local, state, and federal regulatory and statutory requirements including Americans with Disabilities Act (ADA) mandates.



Approve and Disseminate

Staff the plan through the organization's official approval process. This will ensure all relevant staff have input and organization-wide support before senior leadership approval. Once approved, ensure widest dissemination possible using various communication channels. The next step is to begin training and exercising the plan.

Planning Step - 6

Training and Exercise

Train

After an Emergency Action Plan is approved and disseminated, organizations should train their personnel so they have the knowledge, skills, and abilities to perform the tasks identified in the plan. Training can be accomplished in a variety of ways including new employee orientation, "All Hands" meetings, conferences and workshops, newsletters and internal broadcasts, and online courses.

Describe ways your organization can train.

Useful FEMA Online Independent Study Courses

IS 906
Workplace Security Awareness

IS 907
Active Shooter: What You Can Do

IS 914
Surveillance Awareness: What You Can Do

IS 915
Protecting Critical Infrastructure Against Insider Threat

Exercise

Evaluating the effectiveness of plans involves a combination of training events and exercises to determine whether the goals, objectives, decisions, actions, and timing outlined in the plan led to a successful response. Conducting regular exercises help organizations discover resource gaps, develop individual performance, improve coordination with local, state, and federal partners, and identify opportunity for improvement. FEMA's Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs. Organizations can use HSEEP to develop, execute, and evaluate exercises that address their Active Shooter preparedness.

In addition, the DHS Sector-Specific Tabletop Exercise Program (SSTEP) provides an exercise planning resource to assist critical infrastructure owners and operators design their organization's tabletop exercise. Contact the Stakeholder Readiness and Exercise Section at sopd.exercise@hq.dhs.gov for more information.

Develop a time line to accomplish the milestones displayed to the right. Leveraging this "crawl, walk, run" method helps organizations prepare their staff and improve their plan.

Remember – Planning is a Process of Continuous Improvement.